In The Claims:

The claims of the application have been amended herein as indicated in the following marked-up copies of the claims:

1. (currently amended) A method for securely sharing data with authorized parties, wherein the data to be shared is stored in a <u>data store</u> ~~database~~ in a first encrypted format, the method comprising:

    providing a <u>reconfigurable</u> ~~programmable~~ logic device for <u>bridging data transfers between a processor that requests the data transfers and the data store;</u> ~~connection to the database,~~

    _____ ~~wherein~~ the <u>reconfigurable</u> ~~programmable~~ logic device ~~is configured to (1) receive~~ <u>receiving</u> a stream of encrypted data from the <u>data store;</u> ~~database, (2)~~

    _____ <u>the reconfigurable logic device</u> decrypt<u>ing</u> the received encrypted data stream to create decrypted data<u>;</u>

    _____ <u>the reconfigurable logic device,</u> ~~and (3)~~ encrypt<u>ing</u> the decrypted data in a second encrypted format<u>;</u> and

    sharing the data of the second encrypted format by communicating it to an authorized party<u>;</u>

    _____ <u>wherein the decrypted data is not accessible to the processor.</u>

2. (original) The method of claim 1 further comprising:

    providing the authorized party with a key to decrypt the shared data.

3. (original) The method of claim 1 wherein the second encrypted format is different than the first encrypted format such that the key provided to the authorized party will be different than a key necessary to decrypt the stored data.

4. (currently amended) The method of claim 1 further comprising providing a memory device in communication with the <u>reconfigurable</u> ~~programmable~~ logic device, wherein the content of the memory device is accessible only by the programmable logic device, and wherein the <u>reconfigurable</u> ~~programmable~~ logic device is further configured to store at least a portion of the decrypted data in the memory device.

5. (currently amended) The method of claim 1 wherein the <u>data store</u> ~~database~~ is owned by a first party, and wherein the data stored in the <u>data store</u> ~~database~~ is owned by a second party.

6. (currently amended) The method of claim 2 further comprising:

receiving a request for stored data from the authorized party;

responsive to the received request, retrieving stored data from the <u>data store</u> ~~database~~; and

processing the <u>retrieved</u> ~~stored~~ data through the <u>reconfigurable</u> ~~programmable~~ logic device <u>to perform the decrypting and encrypting steps</u>.

7. (currently amended) The method of claim 1 further comprising storing data in the <u>data store</u> ~~database~~ in the first encrypted format.

8. (currently amended) The method of claim 1 wherein the <u>reconfigurable</u> ~~programmable~~ logic device is an FPGA.

9. (currently amended) A device for preparing stored encrypted data for communication to a party, the device comprising:

a <u>reconfigurable</u> ~~programmable~~ logic device ~~in communication with~~ <u>for bridging data transfers between a processor that requests the data transfers and</u> a data <u>store</u> ~~storage medium~~, the data <u>store</u> ~~storage medium~~ comprising data stored therein in a first encrypted format, the <u>reconfigurable</u> ~~programmable~~ logic device being configured to (1) <u>receive a stream of encrypted data from the data store, (2)</u> decrypt ~~a stream of~~ the received encrypted data ~~stream received from the data storage medium~~ to ~~thereby~~ create decrypted data, and ~~(2)~~ <u>(3)</u> encrypt the decrypted data in a second encrypted format<u>, the data encrypted in the second encrypted format for sharing with an authorized party, and wherein the decrypted data is not accessible to the processor</u>.

10. (original) The device of claim 9 wherein the second encrypted format is different than the first encrypted format such that a key provided to the party to decrypt the data of the second encrypted format will be different than a key necessary to decrypt the stored data.

11. (currently amended) The device of claim 9 further comprising the processor, wherein the device is in communication with a processor, the processor being configured to send a request to the device for stored data, the request to be fulfilled at least in part by the programmable logic device, the device further comprising and a memory device in communication with the reconfigurable programmable logic device, wherein the content of the memory device is accessible by the reconfigurable programmable logic device but is not accessible by the processor, wherein the processor is configured to send a request for stored data, the request to be fulfilled at least in part by the reconfigurable logic device, and wherein the reconfigurable programmable logic device is further configured to store at least a portion of the decrypted data in the memory device.

12. (currently amended) The device of claim 9 wherein the reconfigurable programmable logic device is also configured to perform a socket operation on incoming and outgoing data to interface the reconfigurable programmable logic device with upstream and downstream components.

13. (currently amended) The device of claim 9 wherein the data store storage medium comprises a hard disk drive system, the device further comprising a disk connector for interfacing the device with the hard disk drive system.

14. (currently amended) The device of claim 13 further comprising a disk controller in communication with the disk connector and the reconfigurable programmable logic device.

15. (currently amended) The device of claim 14 further comprising an internal bus connecting the disk controller with the reconfigurable programmable logic device.

16. (original) The device of claim 15 wherein the internal bus is a PCI-X bus.

17. (currently amended) The device of claim 16 further comprising a bus connector for interfacing the reconfigurable programmable logic device with a bus on a computer motherboard.

18. (original) The device of claim 17 wherein the bus connector is a PCI-X bus connector.

19. (currently amended) The device of claim 12 wherein the <u>reconfigurable</u> ~~programmable~~ logic device is an FPGA.

20. (currently amended) A method for securely sharing data, wherein the data to be shared is stored in a <u>data store</u> ~~database~~ in a first encrypted format, the method comprising:

providing a reconfigurable logic device for connection to the <u>data store</u> ~~database~~, wherein the <u>reconfigurable</u> ~~programmable~~ logic device is configured to (1) receive a stream of encrypted data from the <u>data store</u> ~~database~~, and (2) using reconfigurable hardware logic, translate the received stream from the first encrypted format to a second encrypted format different than the first encrypted format<u>;</u>

<u>processing the encrypted data stream through the reconfigurable logic device to perform the translation such that a plain text of the encrypted data is not accessible to a processor in communication with the reconfigurable logic device</u>; and

delivering the data of the second encrypted format to a requester.

21. (currently amended) The method of claim 20 wherein the requester is an authorized requester, the method further comprising:

providing the authorized requester with a <u>key</u> ~~means~~ for decrypting the delivered data.

22. (currently amended) The method of claim 20 wherein the <u>data store</u> ~~database~~ is owned by a first party, and wherein the data stored in the <u>data store</u> ~~database~~ is owned by a second party.

23. (currently amended) The method of claim 20 wherein the reconfigurable logic device is an FPGA, the method further comprising:

receiving a request for stored data from the requester;

responsive to the received request, retrieving stored data from the <u>data store</u> ~~database~~; and

<u>wherein the processing step comprises</u> processing the <u>retrieved</u> ~~stored~~ data through the <u>reconfigurable</u> ~~programmable~~ logic device <u>to perform the translation such that the plain text of the encrypted data is not accessible to the processor.</u>

Claims 24-44:   CANCELED.

45. (new) The device of claim 9 wherein the reconfigurable logic device includes internal memory that is not accessible to the processor, and wherein the reconfigurable logic device is further configured to store the decrypted data only in its internal memory.

46. (new) The device of claim 9 further comprising a processing board on which the reconfigurable logic device is deployed, the processing board in communication with the processor and the data store via a system bus, the processing board further comprising a memory device that is not accessible to the processor, wherein the reconfigurable logic device is further configured to store the decrypted data only in the memory device.

47. (new) The device of claim 9 further comprising a processing board on which the reconfigurable logic device is deployed, wherein the reconfigurable logic device includes internal memory that is not accessible to the processor, the processing board in communication with the processor and the data store via a system bus, the processing board further comprising a memory device that is not accessible to the processor, and wherein the reconfigurable logic device is further configured to store a portion of the decrypted data in its internal memory and store another portion of the decrypted data in the memory device.

48. (new) The device of claim 9 wherein the reconfigurable logic device comprises a data processing pipeline, the pipeline comprising a decryption engine and a downstream encryption engine, wherein the reconfigurable logic device performs the decryption operation using the decryption engine and performs the encryption operation using the encryption engine.

49. (new) The device of claim 48 wherein the data processing pipeline further comprises a search engine positioned between the decryption engine and the encryption engine, wherein the search engine is configured to search the decrypted data stream to find a targeted subset of the decrypted data in response to a data request, wherein the encryption engine is configured to perform the encryption operation by encrypting the targeted subset in the second encrypted

format, and wherein the data for sharing comprises the targeted subset encrypted in the second encrypted format.

50. (new) The device of claim 49 wherein the processor comprises a remote processor in communication with the reconfigurable logic device via a network and a network interface, and wherein reconfigurable logic device is further configured to receive the data request from the remote processor.

51. (new) The device of claim 9 wherein the device serves as an access gateway for communication with the data store, the access gateway comprising a system bus, the reconfigurable logic device in communication with the system bus, the processor in communication with the system bus, and a network interface in communication with the system bus, wherein the reconfigurable logic device comprises a Field Programmable Gate Array (FPGA), wherein the network interface is configured to receive a request for data from the data store via a network, and wherein the processor is configured to request that the FPGA initiate the data transfer in response to the request received by the network interface.

52. (new) The device of claim 9 wherein the reconfigurable logic device comprises a programmable logic device.

53. (new) A device for preparing stored encrypted data for communication to a party, the device comprising:
        a reconfigurable logic device for bridging data transfers between a processor that requests the data transfers and a data store, the data store comprising data stored therein in a first encrypted format, the reconfigurable logic device being configured to (1) receive a stream of encrypted data from the data store, (2) decrypt the received encrypted data stream to create decrypted data, wherein the decrypted data is not accessible to the processor, (3) perform a search operation within the decrypted data to locate a targeted subset of data, and (4) encrypt the targeted data subset in a second encrypted format, the targeted data subset encrypted in the second encrypted format for sharing with an authorized party.

54. (new) The device of claim 53 further comprising the processor, wherein the processor is configured to communicate a search query request for the targeted data subset to the reconfigurable logic device, the search query request comprising a specification of a data key for use in the search operation.

55. (new) The device of claim 53 wherein the device serves as an access gateway for communication with the data store, the access gateway comprising a network interface in communication with the reconfigurable logic device, the network interface configured to receive a search query request from the processor via a network and provide the received search query request to the reconfigurable logic device, the search query request comprising a specification of a data key for use in the search operation.

56. (new) The device of claim 53 wherein the reconfigurable logic device comprises a data processing pipeline, the pipeline comprising a decryption engine, a downstream encryption engine and a search engine positioned between the decryption engine and the encryption engine, wherein the reconfigurable logic device performs the decryption operation using the decryption engine, performs the search operation using the search engine and performs the encryption operation using the encryption engine.

57. (new) The method of claim 1 wherein the reconfigurable logic device includes internal memory that is not accessible to the processor, the method further comprising:
    the reconfigurable logic device storing the decrypted data only in its internal memory.

58. (new) The method of claim 1 wherein the reconfigurable logic device is deployed on a processing board, the processing board in communication with the processor and the data store via a system bus, the processing board comprising a memory device that is not accessible to the processor, the method further comprising:
    the reconfigurable logic device storing the decrypted data only in the memory device.

59. (new) The method of claim 1 wherein the reconfigurable logic device includes internal memory that is not accessible to the processor, wherein the reconfigurable logic device is deployed on a processing board, the processing board in communication with the processor and

the data store via a system bus, the processing board further comprising a memory device that is not accessible to the processor, the method further comprising:

the reconfigurable logic device storing a portion of the decrypted data in its internal memory and storing another portion of the decrypted data in the memory device.

60. (new) The method of claim 1 wherein the reconfigurable logic device comprises a data processing pipeline, the pipeline comprising a decryption engine and a downstream encryption engine, wherein the reconfigurable logic device performs the decrypting step using the decryption engine and performs the encrypting step using the encryption engine.

61. (new) The method of claim 60 wherein the data processing pipeline further comprises a search engine positioned between the decryption engine and the encryption engine, wherein the method further comprises:

the search engine searching the decrypted data stream to find a targeted subset of the decrypted data in response to a data request;

wherein the encryption step comprises the encryption engine encrypting the targeted subset in the second encrypted format, and wherein the shared data comprises the targeted subset encrypted in the second encrypted format.

62. (new) The method of claim 61 wherein the processor comprises a remote processor in communication with the reconfigurable logic device via a network and a network interface, the method further comprising the reconfigurable logic device receiving the data request from the remote processor.

63. (new) The method of claim 1 wherein the reconfigurable logic device is part of an access gateway, the access gateway comprising a system bus, the reconfigurable logic device in communication with the system bus, the processor in communication with the system bus, and a network interface in communication with the system bus, wherein the reconfigurable logic device comprises a Field Programmable Gate Array (FPGA), the method further comprising:

the network interface receiving a request for data from the data store via a network; and

the processor requesting that the FPGA initiate the data transfer in response to the request received by the network interface.

64. (new) The method of claim 1 wherein the reconfigurable logic device comprises a programmable logic device.